Bring your own device (BYOD) trends and audit considerations

SIFMA IT audit session

4 October 2012
Disclaimer
Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited located in the US.

This presentation is © 2012 Ernst & Young LLP. All rights reserved. No part of this document may be reproduced, transmitted or otherwise distributed in any form or by any means, electronic or mechanical, including by photocopying, facsimile transmission, recording, rekeying or using any information storage and retrieval system, without written permission from Ernst & Young LLP. Any reproduction, transmission or distribution of this form or any of the material herein is prohibited and is in violation of US and international law. Ernst & Young and its member firms expressly disclaim any liability in connection with use of this presentation or its contents by any third party.

The views expressed by panelists are not necessarily those of Ernst & Young LLP.

Circular 230 disclaimer
Any US tax advice contained herein was not intended or written to be used, and cannot be used, for the purpose of avoiding penalties that may be imposed under the Internal Revenue Code or applicable state or local tax law provisions.

These slides are for educational purposes only and are not intended, and should not be relied upon, as accounting advice.
Agenda

► Overview
► Evolution of the IT environment
► Benefits of BYOD
► Challenges
► Implementation considerations
► Mobile device management
► BYOD risks and controls
► Mobile security leading practices
Overview

► BYOD is a strategy in which organizations allow employees to use their personal devices to access company resources.
► Increased functionality, such as HR reporting, expense reporting, sales-force automation, customer relationship management (CRM), and asset management on employee devices.
► BYOD extends the range of the company “network” and is a result of the consumerization of IT – IT’s emergence in the consumer market increases personal technology being pulled into the organization.
Evolution of the IT environment

<table>
<thead>
<tr>
<th>2006</th>
<th>2008</th>
<th>2010</th>
<th>2012</th>
</tr>
</thead>
<tbody>
<tr>
<td>Achieving success in a globalized world</td>
<td>Moving beyond compliance</td>
<td>Borderless security</td>
<td>Information security re-invented</td>
</tr>
<tr>
<td>➤ More third-party relationships</td>
<td>➤ Brand protection</td>
<td>➤ Mobile computing</td>
<td>➤ Need for a fundamental shift in information security</td>
</tr>
<tr>
<td>➤ Focus on privacy and data protection</td>
<td>➤ IP</td>
<td>➤ Cloud computing</td>
<td>➤ Integration and coordination</td>
</tr>
<tr>
<td>➤ Business continuity</td>
<td>➤ Operational risk</td>
<td>➤ Social media</td>
<td>➤ Data is everywhere</td>
</tr>
<tr>
<td>➤ Operational risk</td>
<td></td>
<td>➤ Mobile computing</td>
<td></td>
</tr>
</tbody>
</table>

Need for change

Source: Ernst & Young 2012 Global Information Security Survey (GISS) – information security re-invented
2012 Global Information Security Survey* – keeping track of mobile computing

Does your organization currently permit the use of tablet computers for business use?

<table>
<thead>
<tr>
<th>Option</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>No, and no plans to use in the next 12 months</td>
<td>4.85%</td>
</tr>
<tr>
<td>No, but planned within the next 12 months</td>
<td>6.47%</td>
</tr>
<tr>
<td>*Tablets are under evaluation or very limited use</td>
<td>35.28%</td>
</tr>
<tr>
<td>Yes, company-owned tablets devices are widely in use</td>
<td>18.12%</td>
</tr>
<tr>
<td>Yes, private-owned tablets widely in use but not supported by the organization</td>
<td>13.92%</td>
</tr>
<tr>
<td>Yes, private-owned tablets widely in use and supported by the organization by means of a Bring Your Own Device (BYOD) policy</td>
<td>21.36%</td>
</tr>
</tbody>
</table>

Increased adoption and shift in responses from the 2011 survey, with more than 85% of respondents indicating an interest in BYOD with varying levels of adoption.

*US responses only
BYOD high-level technology landscape

BYOD devices pose the challenge of connecting to corporate servers by transferring data over both secured and unsecured networks:

- **Non-MDM (mobile device management) enabled BYOD devices**
- **MDM enabled BYOD devices**
- **Corporate wifi networks**
- **Non-corporate wifi networks**
- **Wireless carrier networks**
- **Internet (unsecured networks)**
- **Corporate servers (email, application, etc.)**
- **Corporate firewall**
Benefits of BYOD

► Enhanced collaboration and mobility
► Expanded mobile access to resources
► Increased employee moral and business productivity
► Reduced spending on procurement, training and support of devices as well as the responsibility for device life cycle management
► Relieving IT of the responsibility of managing service plans
► Implementation process can be shared with end users – allow users to self-enroll
► Operational cost savings through consolidated delivery mechanisms
Challenges

► Data security
► Separating personal data from enterprise data
► Changing culture – more flexibility for employees, reduced control for the IT department
► New considerations when designing the IT strategy and implementing security policies; aligning user needs and business requirements such as security, HR, legal, availability, integrity
► Definition of the responsibility for device maintenance cycle
► Managing an increasing application entitlement inventory
► Financial industry regulatory requirements requiring supervision and archiving
Challenges

► Blurring of work-life boundaries and employee burnout
► Identity management strategy, given that each employee may have multiple devices connecting to the enterprise network
► Monitoring performance and capacity becomes more complicated, given that the IT environment is more dynamic
► Modeling and forecasting system performance becomes more difficult, because the number of devices used is no longer controlled by the organization
► Users may be reluctant to participate due to concerns regarding privacy
BYOD implementation considerations

► A BYOD program that is device agnostic can utilize virtual environments and network segmentation to limit the impact radius of events
► Separate secure network for BYOD devices – similar to guest network
► Acceptable usage agreements
► Does the organization collect data from employee-owned devices? What data is collected and how is it used? Is it personally identifiable information?
► Data classification and user classification
► A fundamental security component of a BYOD infrastructure is the addition of an MDM (mobile device management) solution
MDM

- Centralized mobile device management allows IT departments to set company-wide policies.
- Over the air programming allows the IT department to remotely configure devices connected to the network.
- MDM can be used to allow the preapproval of certain applications i.e., white listing.
- MDM can be deployed using software as a service or housed internally.
BYOD risks and controls

- Mobile devices share many of the same risks as stem from the use of laptops.
- Mobile devices and networks often contain stronger client-side controls that shift the focus away towards device lockdown.
## BYOD risks and controls

<table>
<thead>
<tr>
<th>Scope</th>
<th>Risk</th>
<th>Potential controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Inadequate policies to define acceptable usage</td>
<td>BYOD policies outlining the actions end users must take to prevent the misuse or loss of corporate information, monitoring and oversight over enforcement of corporate controls</td>
</tr>
<tr>
<td></td>
<td>Noncompliance with regulatory requirements (e.g., records of communications by an employee pertaining to the firm’s business must be maintained, retrievable and reviewed consistent with SEC Rules 17a-3 and 17a-4 and NASD Rule 31101)</td>
<td></td>
</tr>
<tr>
<td>Network security</td>
<td>The device is lost/stolen and used to gain access to the corporate network</td>
<td>Two factor authentication is used for remote access. Networks for mobile devices are segmented from the corporate network</td>
</tr>
</tbody>
</table>
## BYOD risks and controls

<table>
<thead>
<tr>
<th>Scope</th>
<th>Risk</th>
<th>Potential controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy</td>
<td>Company destroys or corrupts personal data</td>
<td>Selective remote wipe, disk partitioning and virtualization are implemented on devices.</td>
</tr>
<tr>
<td></td>
<td>Personally identifiable information is collected without a business requirement</td>
<td></td>
</tr>
<tr>
<td>Logical access</td>
<td>Devices not in compliance access the network, internal application or database</td>
<td>Updates are required to connect to the network; installs are pushed out regularly.</td>
</tr>
<tr>
<td>Device security</td>
<td>The device is lost or stolen and unauthorized users access sensitive company data</td>
<td>Technology controls such as encryption, remote wiping, PIN and password lockout are enforced on the mobile devices.</td>
</tr>
</tbody>
</table>
## 2012 Global Information Security Survey* – keeping track of mobile computing

Controls implemented to mitigate the new or increased risks related to the use of mobile computing

<table>
<thead>
<tr>
<th>Control</th>
<th>US Responses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy adjustments</td>
<td>68.93%</td>
</tr>
<tr>
<td>New mobile device management software</td>
<td>58.90%</td>
</tr>
<tr>
<td>New disciplinary processes</td>
<td>6.15%</td>
</tr>
<tr>
<td>Increased security awareness activities</td>
<td>48.87%</td>
</tr>
<tr>
<td>Increased auditing capability</td>
<td>16.50%</td>
</tr>
<tr>
<td>Governance process to manage the use of mobile applications</td>
<td>46.60%</td>
</tr>
<tr>
<td>Encryption techniques</td>
<td>51.78%</td>
</tr>
<tr>
<td>Disallow the use of all tablets / smartphones for professional use</td>
<td>2.91%</td>
</tr>
<tr>
<td>Architectural changes</td>
<td>37.22%</td>
</tr>
<tr>
<td>Attack &amp; Penetration testing of mobile applications</td>
<td>13.92%</td>
</tr>
<tr>
<td>Allow the use of company-owned devices, but disallow use of personal devices</td>
<td>25.57%</td>
</tr>
<tr>
<td>Adjusted incident management processes</td>
<td>17.48%</td>
</tr>
</tbody>
</table>

*US responses only
Data loss and BYOD

- BYOD poses unique challenges to organizations and monitoring of mobile computing activity
  - Loss of control over information “containers” (devices)
  - Companies must focus on protecting the data itself by employing data loss prevention (DLP) techniques
    - File encryption (for data in motion and static)
    - Monitoring of outbound transmissions (monitoring controls for email, restrictions against transferring data to locations other than authorized devices, etc.)
- Regulatory requirements for monitoring activities. For example:
  - SEC rules 17a-3 and 17a-4 and NASD Rule 31101 – records of firm-related business communications made by an employee must be maintained, retrievable and reviewed
  - NASD2210 – communication with the public
Mobile security — leading practices

- Data on devices
  - Locked-down applications
  - Mobile device management for enforcing encryption and remote wipe

- Remote exploits
  - Threat intelligence
  - Monitor vendor firmware updates
  - Mobile device management software to monitor device firmware compliance

- Communications
  - Encrypted inbound and outbound communications
  - Enforced for applications as well as access into corporate network
Mobile security — leading practices

- **Installed applications**
  - Mobile device management software to restrict application installation
  - Restrict which “app store” can be used
  - Due diligence for applications purchased for corporate use

- **Creating applications for mobile devices**
  - Threat modeling
  - Secure software development life cycle (SDLC) tollgates
  - Secure backend infrastructure

- **BYOD**
  - Enforce minimum supported security baseline configuration
  - Corporate functionality on devices should be kept to a minimum
What does this mean for your organization?

► The number of mobile workers worldwide is expected to reach 1.3b by 2015 (Sources: *Inside Telecommunications*, issue 6. Quarterly talking points from Ernst & Young's Global Telecommunications Center)

► Consumer obsession with technology will intensify as manufacturers design and deliver more progressive devices with increased computing power.

► Denial of the BYOD trend is no longer an option.

► To successfully transition or institute a BYOD infrastructure, it’s critical to understand the confluence of necessary technologies, governance, policies and processes.
Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 167,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

Ernst & Young is a leader in serving the global financial services marketplace

Nearly 35,000 Ernst & Young financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, Ernst & Young is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 4,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

Ernst & Young professionals in our financial services practices worldwide align with key global industry groups, including Ernst & Young's Global Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, Ernst & Young's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

It's how Ernst & Young makes a difference.

© 2012 Ernst & Young LLP.
All Rights Reserved.
1209-1346913 NY

ED 10 Sep 2014